US application number 10511775

# RESPONSE TO OFFICE ACTION

This paper responds to the Office Action dated May 14, 2008.

## Novelty

The Examiner contends that claims 1, 2 and 6 are supposedly anticipated by Vaidya. However, it is submitted that the prior-art arrangement is distinct and distinguishable from the invention as currently claimed.

Indeed, it is submitted that the arrangement disclosed in Vaidya falls squarely within the category of known 'misuse detection' systems as described in the present application:

> The misuse paradigm is straightforward in the sense that the … IDS has some knowledge of suspicious behaviour and looks for actions that match this knowledge. Such knowledge is typically represented as a set of signatures, where each signature encapsulates the salient features of a different attack or class of attack.

(Page 1, para 4.) In particular, the arrangement disclosed in Vaidya does not feature the use of "general rules" as featured in current claims 1, 2 and 6. The Examiner suggests that Vaidya's attack signature profiles equate to general rules because they can be "generic" (i.e. can describe attacks which are common to most networks).

However, while Vaidya's use of the term "generic" refers to the target networks associated with a particular (type of) attack, a "general rule" encodes knowledge concerning the impact and/or function of a particular (type of) attack.

The "general rules" of the present invention "consider what the result of the input to the computer will be rather than what it looks like" (page 2 paragraph 19). In other words, the "general rules" of the present invention predict and preempt dangerous functions by encoding contextual and behavioral (i.e. semantic) knowledge. This point is repeated at page 2 paragraph 17:

> the present invention … creates an IDS that searches computer input traffic in a semantic matching manner to determine the contextual function of the traffic, as opposed to simple

signature matching of known sinister traffic (or syntactic matching).

Thus, the general rules of the current invention represent knowledge regarding the function of input traffic rather than simply describing "the identifiable characteristics" of network intrusions. (Vaidya, column 3 lines12 to 15). Thus, "the set of predicates [in the invention as currently claimed] allow a more thorough representation of the facts than may be found in an IDS rule set" (page 5 paragraph 70).

Additionally, as the Vaidya arrangement comprises signature profiles rather than general rules, Vaidya does not disclose means for "comparing, in a semantic manner, sets of actions forming [an] activity against ... one or more general rules to identify an intrusion or attempted intrusion". The matching performed by Vaidya is at a syntactic, not semantic, level.

With regards to claim 6, the arrangement disclosed in Vaidya does not disclose a means for "automatically generating and storing in [a] knowledge base new general rules…".

The arrangement of Vaidya requires additional signature profiles (describing a new class of attack) to be integrated into the system through the intervention of a human operator. Indeed, Vaidya states that one advantage of the arrangement is that it facilitates (but does not eliminate the need for) updates. These updates must be made by a human operator. (Vaidya column 3 lines 1 to 11 and 23 to 26).

The need for manual updates is specifically mentioned in the present applicaiton as a disadvantage of misuse-model prior art systems wherein "a substantial amount of human intervention is required in connection with analysis of previous attacks and encapsulation of newly-discovered attacks or classes of attack within a signature to input to the model" (page 1, paragraph 9).

Additionally, the Examiner suggests that Vaidya's creation of new session entries in the state cache equates to the storage of new general rules in the knowledge base. However, this is not correct. The state cache stores (temporary) information for monitoring or tracking the state of an application session while it is currently executing. It does not store (for later retrieval) general rules relating to the impact of functions which may be executed in the future.

Thus, claims 1, 2 and 6 are novel over Vaidya.

## Unobviousness

The Examiner contends that dependent claims 3-5, 7, 9 and 10 are supposedly obvious over a two-way combination of Vaidya and Bratko, which makes known the principles and techniques of Inductive Logic Programming (ILP). The Examiner asserts that knowledge of ILP would lead the skilled addressee to modify Vaidya's arrangement to arrive at the invention as currently claimed.

However, the arrangement disclosed in Vaidya cannot be modified to arrive at the present invention by simply re-implementing it in a logic programming language such as Prolog.

As above, the general rules used in the present invention do not equate to the attack signature profiles of Vaidya. The former performs analysis on a semantic level, while the latter performs syntactic level matching.

Furthermore, Vaidya's attack signature profiles are categorized into three types: simple, sequential or timer/counter. The present arrangement, however, is not constrained to this categorization as it considers the impact of potentially dangerous functions rather than detecting known characteristics associated with types of attack.

Thus, the arrangements approach the problem of intrusion detection from different perspectives. Nothing in Vaidya would lead one skilled in the art to arrive at the present invention, either on its own or in conjunction with the Bratko reference.

**Comments from the inventor.** Inventor Steve Moyle offers some comments which are on the attached pages.

**Conclusion.** Reconsideration is respectfully requested.

Respectfully submitted,
/s/
Carl Oppedahl
PTO Reg. No. 32746